Atty. Docket No. 005313.00003 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Patent Of: Marc Van Heyningen et al.

U.S. Pat. App. No.: 09/783,146

Filed: February 13, 2001

For: Method And Apparatus For Providing Secure Streaming Data Transmission Facilities Using Unreliable Protocols

Examiner: Kambiz Zand

Group Art Unit: 2132

SUPPLEMENTAL APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450,
Alexandria, Virginia 22313-1450

Sir:

Appellants hereby appeal to the Board of Patent Appeals and Interferences from the decision of the Primary Examiner on December 20, 2005, finally rejecting claims 1-51 and 53-58 in the above-captioned patent application.

It is respectfully noted that claim 52 was not rejected or objected to in the final Office Action of December 20, 2005. Accordingly, it is Appellants' understanding that claim 52 has been allowed.

Real Party In Interest

The real party in interest is Aventail Corporation, a U.S. corporation having a place of business in Seattle, Washington.

Related Appeals and Interferences

There are no related appeals or interferences.

Status of Claims

Claims 1-58 (reproduced for reference in the Claims Appendix) are pending in the application, with claims 1, 20, 38 and 47 being independent claims. In a final Office Action dated December 20, 2005, the Primary Examiner rejected each of claims 1-7, 9-20, 22-27, 29, 31-43, 45, 47-51 and 53-58. Claims 8, 21, 28, 30, 44 and 46 were then objected to as containing allowable subject matter but depending from rejected claims. Appellants now appeal from the Primary Examiner's rejection of the pending claims.

As previously noted, claim 52 was not rejected, objected to, or otherwise addressed in the final Office Action of December 20, 2005. Appellants therefore understand that claim 52 stands allowed.

Status of Amendments

No amendments have been made to the claims following the final Office Action of December 20, 2005.

Summary of Claimed Subject Matter

The claims are directed to the secure transmission of data over a computer network. With various examples of the invention, a first computer, such as a client computer 301, communicates with a second computer, such as a proxy server 302. The client computer 301 may, for example, securely establish a communication path with the proxy server 302 through a

SOCKS client 301B. (See, e.g., the specification, page 11, lines 20-24, and Fig. 3.) The client computer 301 encrypts data records 507 by encrypting plaintext 501 into ciphertext using an encryption function 508, such as the conventional DES encryption algorithm. Each plaintext 501 may be encrypted using a session key 502, a nonce value 504 and an initialization vector 503, which may be random numbers. The nonce value 504 and an initialization vector 503 used to encrypt the plaintext 501 are then included in the data record 507. Thus, each data record 507 is encrypted without reference to a previous encrypted data record 507. (*Id.*, page 15, lines 3-12, and Figs. 5A and 5B.)

The data records 507 are transmitted to the second computer using an unreliable communication protocol, such as the User Datagram Protocol (UDP). (See, *Id.*, page 14, lines 22-28.) Upon receiving a data record 507, the second computer uses the initialization vector 503 and the nonce value 504 included with the data record 507 to decrypt the ciphertext without reference to a previously received data record 507. (*Id.*, page 15, lines 13-16, page 15, line 27 to page 16, line 5, and Figs. 5A and 5B.)

The proxy server 302 transmits session information for the communication session with the client computer 301 to a third computer, such as another proxy server 302. (See, e.g., *Id.*, page 19, line 18 to page 20, line 3, page 21, lines 13-17, etc., and Fig. 7.) The session information may include all of the information necessary for the third computer to resume the communication session between the first computer and the second computer, such as the session key 502, a peer certificate used to authenticate the client computer 301, a session identifier, a cipher specification, a method authentication check algorithm used for the communication session, and the like. (*Id.*, page 20, lines 5-21.)

Grounds Of Rejection To Be Reviewed On Appeal

The following grounds of rejection are presented to the Board of Patent Appeals and Interferences for review in this appeal:

(a) Claims 1, 20, 38 and 47 have been provisionally rejected under the judicially created doctrine of obviousness-type double patenting over claims 1, 10, 16, and 23 of copending U.S. Patent Application No. 09/782,593;

(b) Claims 1-4, 10-12, 15, 16, 20, 24, 25, 27, 29, 33, 34, 38, 39, 43, 45, 47, 48, 54, 56 and 57 have been rejected under 35 U.S.C. §102(e) over U.S. Patent No. 6,216,229 to Fischer;

(c) Claims 5-7, 22, 23, and 49-51 have been rejected under 35 U.S.C. §103 over U.S. Patent No. 6,216,229 to Fischer in view of U.S. Patent No. 6,317,729 to Camp et al.;

(d) Claims 9, 13, 14, 17-19, 24, 26, 31, 32, 35-37, 40-42, 53, 55, and 58 have been rejected under 35 U.S.C. §103 over U.S. Patent No. 6,216,229 to Fischer in view of prior art allegedly disclosed in Applicant's specification.

Arguments

The Provisional Rejection Of Claims 1, 20, 38 and 47 Under The
Judicially Created Doctrine Of Obviousness-Type Double Patenting Is Improper

In the Office Action, the Primary Examiner provisionally rejected claims 1, 20, 38 and 47 under the judicially created doctrine of obviousness-type double patenting over claims 1, 10, 16 and 23 of copending U.S. Patent Application No. 09/782,593. Appellants respectfully traverse this rejection, and courteously ask for its reversal.

Applicants courteously urge that the subject matter of claims 1, 20, 38 and 47, are, in fact, patentably distinct from the subject matter of claims 1, 10, 16 and 23 currently pending in U.S. Patent Application No. 09/782,593. For example, claim 1 of this application recites that the second computer, which receives and decrypts data records transmitted from the first computer, transmits session information for encrypting and decrypting the data records to a third computer. As expressly recited by the Primary Examiner, this feature is not recited by any of claims 1, 10, 16 and 23 of U.S. Patent Application No. 09/782,593. (See final Office Action, page 5, lines 26-28.)

Similarly, claim 20 of this application recites that the proxy server transmits session information including the previously shared encryption key for use in decrypting the plurality of data records to another server. Claim 38 then recites a third computer coupled to the second computer and having a cache memory for storing at least the encryption key, while claim 47 recites transmitting session information for decrypting the encrypted data records to a second computer. These features likewise are not recited by any of claims 1, 10, 16 and 23 in U.S. Patent Application No. 09/782,593.

In support of this rejection, the Primary Examiner simply has concluded that the features absent from the claims of U.S. Patent Application No. 09/782,593 are obvious. Unfortunately, the Primary Examiner has provided no basis for this conclusion, either in the prior art or by a reasoned analysis of the routine knowledge of one of ordinary skill in the art. For example, in rejecting the independent claims, the Examiner merely argued that:

> [I]t would have been obvious to one of ordinary skill in the art to transmit session information to another computer for the purpose of backup or secure transmission of data records. (See Office Action, page 5, line 28 to page 6, line 2, page 6, lines

7-9, lines 13-15, and page 7, lines 5-7.)

The Examiner has not explained, however, why one of ordinary skill in the art would bother to obtain a backup of session information for encrypting and decrypting communications between two computers, much less why one of ordinary skill in the art would make that backup by transmitting the session information to a third computer, rather than simply storing it in a remote storage device, such as a hard drive. Similarly, the Examiner has provided no reasoning to explain how storing the session information on a third computer would provide secure transmission of data records. Presumably, one of ordinary skill in the art would understand that the encrypted communication between the first computer and the second computer would provide secure transmission of data records without ever involving a third computer.

In the final Office Action, the Primary Examiner attempted to address this deficiency by arguing that the transmission of the session information to a third computer is only a design choice for intended use:

> The addition of the third computer and transmission of session information to it by the second computer does not change the fact that the process of passing the information for encryption and decryption is repeated process [sic] that it is taken [sic] place between the first two computers and such a [sic] addition is only a design choice for intended use. (*Id.*, page 2, line 17 to page 3, line 3.)

The Primary Examiner also argues that:

> The preamble of the claims involve [sic] refers to computer network [sic], therefore it would have been obvious to one of ordinary skilled [sic] in the art at the time the invention was made to transmit the session information from one computer to another (example, from second to the third; or first to the second or vice versa or to other terminals in the system network) in order to enable the receiving terminal capabilities for decryption of the encrypted records receive [sic] or vice versa. Such motivation is obvious *since without transfer of such session information the received terminal in unable to perform decryption of the encrypted records received*. (*Id.*, page 3 lines 3-11, *emphasis added*.)

The Primary Examiner's reasoning ignores conventional communication techniques, however. Typically, encryption information from a secure communication session is intentionally not shared among terminals in a computer network, in order to maintain the security of that communication session.

Instead, to ensure privacy, terminals that will participate in a secure communication session are provided the necessary encryption information in advance, or negotiate the encryption information at the beginning of the communication session. The Primary Examiner's alleged obvious "motivation," emphasized above, can only be predicated upon a review of the features of the invention disclosed in Appellants specification, and thus is impermissible hindsight.

Accordingly, Appellants again respectfully submit that the Examiner has not made out the *prima facie* showing of obviousness required to sustain the outstanding obviousness-type double patenting rejection of claims 1, 20, 38 and 47. Further, Applicants courteously urge that claims 1, 20, 38 and 47 are patentably distinct from the subject matter of claims 1, 10, 16. It is therefore requested that the outstanding rejection of claims 1, 20, 38 and 47 under the judicially created doctrine of obviousness-type double patenting be reversed.

The Rejection Of Claims 1-4, 10-12, 15, 16, 20, 24, 25, 27, 29, 34, 38, 39, 43, 45, 47, 48, 54, 56 and 57 Under 35 U.S.C. §102(e) Over U.S. Patent No. 6,216,229 To Fischer Is Improper

Claims 1-4, 10-12, 15, 16, 20, 24, 25, 27, 29, 34, 38, 39, 43, 45, 47, 48, 54, 56, and 57 were rejected under 35 U.S.C. §102(e) over U.S. Patent No. 6,216,229 B1 to Fischer. Appellants respectfully traverse this rejection, and courteously ask for its withdrawal as well.

Claims 1-4, 10-12, 15, 16, 20, 24, 25, 27, 29, 34, 38, 39, 43, 45, 47, 48, 54, 56, And 57

As previously noted, each of the method claims in this application generally relate to a process of (1) transmitting encrypted data records between two computers during a communication session, and (2) providing session information for decrypting the records to another computer (i.e., a computer outside of that communication session). The apparatus claims similarly recite (1) a first computer that uses an encryption key to encrypt and send data records to a second computer, which decrypts the data records using the decryption key, and (2) a third computer storing the encryption key.

Appellants respectfully submit that the Fischer patent does not teach or suggest these recited features of the invention. The Fischer patent is directed toward a technique for preventing unauthorized access to secret information provided to an escrow trustee. As discussed in the Fischer patent, a user initially encrypts an escrow record with the secret information. (See column 9, lines 38-42.) This escrow record is then transmitted to the escrow trustee. (See, e.g., *Id*., lines 59-61.) When an authorized user subsequently needs to retrieve the secret information, the escrow trustee decrypts the escrow record. (See column 10, lines 37-51.) If credential information provided by the user is authentic, then the escrow trustee re-encrypts the secret information using new encryption information (i.e., a public key included in the escrow record or provided by the user), and forwards the re-encrypted secret information to the user. (See column 11, lines 11-17.)

Notably, the escrow trustee of the Fischer patent does not provide the encryption information (i.e., the information used to encrypt the secret information) to anyone, much less a third computer. Moreover, while the Fischer patent discloses that the user and the escrow trustee

may be computer terminals in a larger network, the actual escrow procedure described in the Fischer patent does not involve a third computer in any way.

In the final Office Action, the Primary Examiner additionally referred to the portion of the Fischer patent at column 5, lines 34-42, which refers to split-key secret sharing. (Final Office Action, page 4, lines 14-18.) Appellants point out that the term "split-key," as used in the Fischer patent, refers to a division of the secret information into multiple parts, and not to encryption information used to encrypt the secret information. Appellants respectfully invite the Board's attention to the portion of the Fischer patent at column 8, lines 15-22, which explains in more detail:

> Alternatively, the secret information may be "split" if the secret is being split among multiple trustees. In the case of "split" information, there will be multiple escrow components created - *encrypted under respective public keys of each different trustee*. Split escrowing can require that information must be retrieved from several trustees, and then combined in order to be able to reconstruct the user's secret. (*Emphasis added*.)

Nothing in the Fischer patent would teach or suggest the sharing of encryption information between different escrow trustees with this type of "split key" arrangement.

Claims 10, 27, 43, And 54

With particular regard to claims 10, this claim recites that the step of encrypting and transmitting data records is performed by a proxy server that encrypts data records received from another server, while claim 54 recites that the first computer is a proxy server that encrypts data records received from a third computer. Claim 27 and 43 similarly recite the use of a second proxy server. These features also are not taught or suggested by the Fischer et al. patent. In rejecting claims 10, 43, and 54, for example, the Examiner referred generally to Figs. 1-6 of the

Fischer et al. patent, but there is no reference to a proxy server in any of these figures. With regard to claim 27, the Examiner offered no reference to the Fischer et al. patent even purporting to teach or suggest the use of a second proxy server.

Claim 11

Claim 11 then recites that a third computer encrypts and transmits data records to the first computer using an unreliable communication protocol. When rejecting this claim, the Examiner simply asserted that the Fischer et al. patent discloses the user of an unreliable communication protocol, but provided no support for this assertion. (See final Office Action, page 9, lines 3-6.) In fact, the Fischer et al. patent does not teach or suggest the use of an unreliable communication protocol. Moreover, because the Fischer et al. patent is directed to safely maintaining escrow information, it is highly doubtful that one of ordinary skill in the art would have been led to employ an unreliable communication protocol with the techniques disclosed in the Fischer et al. patent.

Claim 12

With regard to claim 12, this claim recites that a fourth computer retrieves the session information from the third computer, and encrypts and transmits data records to the first computer by employing the session information. As noted above, the Fischer et al. patent only describes a transaction between a first computer and second computer. It certainly does not teach or suggest a fourth computer retrieving session information from a third computer to securely communicate with a first computer.

Claim 24

With regard to claim 24, this claim recites the use of both the Transmission Control

Protocol and the User Datagram Protocol. The Fischer et al. patent, however, makes no reference to either the Transmission Control Protocol and the User Datagram Protocol. Appellants respectfully point out that the Examiner offered no evidence or argument in the final Office Action to justify this rejection.

Summary

Accordingly, Appellants again urge that the Fischer patent does not teach or suggest the features of the invention recited in claims 1-4, 10-12, 15, 16, 20, 24, 25, 27, 29, 34, 38, 39, 43, and 45. Appellants therefore urge that the Fischer patent does not support the outstanding rejection of these claims under 35 U.S.C. §102(e), and ask that this rejection be reversed.

The Rejection Of Claims 5-7, 22, 23, And 49-51 Under
35 U.S.C. §103 Over U.S. Patent No. 6,216,229 To Fischer
In View Of U.S. Patent No. 6,317,729 To Camp et al. Is Improper

Claims 5-7, 22, 23, and 49-51 were rejected under 35 U.S.C. §103 over the Fischer patent in view of U.S. Patent No. 6,371,729 to Camp et al. Appellants courteously ask that this rejection also be reversed.

Claims 5-7, 22, 23, And 49-51

As discussed in detail above, Appellants again submit that nothing in the Fischer patent teaches or suggests claimed features of the invention. It is respectfully submitted that the Camp et al. patent does not remedy these substantial omissions of the Fischer patent.

The Camp et al. patent is directed to a method for certifying delivery of secure electronic transactions. The Camp et al. patent does not teach or suggest transmitting encrypted data records between two computers during a communication session, and providing session information for decrypting the records to another computer. Further, the Camp et al. patent does

not even teach incorporating a nonce in a data record for use by a second computer in combination with a previously shared encryption key to decrypt the data record.

In making this rejection, the Primary Examiner referred to "…random numbers chall-m and chall-c that corresponds to keys used for encryption or decryption…" (See final Office Action, page 13, lines 2-3.) Appellants point out that the Camp et al. patent alternately refers to the values chall-m and chall-c as "a corresponding once" (column 7, lines 47-48), "a corresponding challenge" (column 8, lines 4-5), "a new challenge from merchant to customer" (column 8, lines 5-6), and "a customer's transaction identifier" (column 8, lines 38-39, lines 64-65, and column 9, lines 43-44). Notwithstanding the ambiguity with which the values chall-m and chall-c are discussed in the Camp et al. patent, nothing in this patent would teach or suggest the use of either of these values to encrypt or decrypt a data record.

Claims 5 And 49

Regarding claims 5 and 49 in particular, these claims recite incorporating a nonce in each data record that is used with a previously shared encryption key to decrypt each data record. The Examiner has supported the rejection of these claims by alleging that this features is disclosed in columns 4-5, table 2, and columns 7-11, stating:

> …random number chall-m and chall-c that corresponds [sic] to keys used for encrypt or decryption… (See final Office Action, page 13, lines 2-3.)

Appellants respectfully point out, however, that there is simply no basis for the Examiner's conclusion. Nothing in the Camp et al. patent would teach or suggest the use of either the value chall-c or the value chall-m with an encryption key to decrypt a data record.

Claims 7 And 51

With regard to claims 7 and 51 in particular, these claims recite verifying that the nonce has not previously been received in a previously transmitted data record. In rejecting these claims, the Examiner broadly alleged that this feature was disclosed in columns 7-11 of the Camp et al. patent. Appellant respectfully points out, however, that the Camp et al. provides no such teaching, either in columns 7-11 or elsewhere in the patent.

Summary

Appellants therefore submit that no combination of the Fischer patent and the Camp et al. patent could teach or suggest the features of the invention recited in any of claims 5-7, 22, 23, and 49-51. Appellants accordingly request that the rejections of claims 5-7, 9, 13, 14, 17-19, 22-24, 26, 31, 32, 35-37, 40, 42 49-51, 53, 55, and 58 be reversed.

The Rejection Of Claims 9, 13, 14, 17-19, 24, 26, 31, 32, 35-37, 40, 42, 53, 55, And 58 Under 35 U.S.C. §103 Over U.S. Patent No. 6,216,229 To Fischer In View Of Prior Art Allegedly Disclosed In Applicant's Specification

Claims 9, 13, 14, 17-19, 24, 26, 31, 32, 35-37, 40, 42, 53, 55, and 58 were rejected under 35 U.S.C. §103 over the Fischer patent in view of prior art allegedly disclosed in Applicants' specification. Appellants respectfully traverse this rejection, and ask for its reversal.

Claims 9, 13, 14, 17-19, 24, 26, 31, 32, 35-37, 40, 42, 53, 55, And 58

Applicants first respectfully point out that the Examiner has not set forth the *prima facie* showing necessary to sustain this rejection. In making this rejection, the only motivation for modifying the teachings of the Fischer et al. patent offered by the Examiner was an express reference to Appellants' own application. (See the final Office Action, page 14, lines 18-20 and page 15, lines 5-7 and lines 13-15.) The Examiner's reliance upon Appellants' specification is clearly impermissible hindsight.

Claims 9, 24, 40, And 53

With particular regard to claims 9, 24, 40, and 53, these claims specifically recite the use of the unreliable User Datagram Protocol. Because the Fischer patent is directed to the safe escrow of data, one of ordinary skill in the art would not have been led to modify the teachings of the Fischer patent to use this unreliable communication protocol.

Summary

Second, as discussed in detail above, nothing in the Fischer patent teaches or suggests claimed features of the invention. It is respectfully submitted that Applicants' specification discloses no prior art that would remedy the omissions of the Fischer patent noted above. Appellants therefore submit that no combination of the Fischer patent and the Prior Art Allegedly Disclosed In Applicant's Specification could teach or suggest the features of the invention recited in any of claims 9, 13, 14, 17-19, 24, 26, 31, 32, 35-37, 40, 42, 53, 55, and 58. Appellants accordingly request that the rejections of these claims be reversed as well.

Conclusion

The rejections made in the final Office Action dated December 20, 2005, should be reversed for at least the reasons recited above. Allowance of claims 1-58 in their entirety is, therefore, respectfully requested.

The Commissioner is authorized to charge the associated small entity fees of; 1.) $250.00 for the filing of the original filing of the Appeal Brief and 2.) $60.00 the for the filing of a Petition for a one month Extension of Time, to Deposit Account No. 19-0733. Should additional

fees be deemed necessary, such fees are hereby requested and the Commissioner is authorized to charge such fees to Deposit Account No. 19-0733 as well.

Respectfully submitted,

BANNER & WITCOFF, LTD.

s/Thomas L. Evans/s
Thomas L. Evans, Reg. No. 35,805

1001 G Street, N.W., 11th Floor
Washington, D.C. 20001-4597
Telephone: (202) 824-3000
Facsimile: (202) 824-3001

Date: January 22, 2007

APPENDIX A - CLAIMS ON APPEAL

1. A method of transmitting data securely over a computer network, comprising the steps of:

(1) establishing a communication path between a first computer and a second computer;

(2) encrypting and transmitting data records between the first computer and the second computer using an unreliable communication protocol, wherein each data record is encrypted without reference to a previously transmitted data record;

(3) in the second computer, receiving and decrypting the data records transmitted in step (2) without reference to a previously received data record; and

(4) in the second computer, transmitting session information for encrypting and decrypting the data records to a third computer.

2. The method of claim 1, further comprising the step of, prior to step (1), establishing a reliable communication path between the first computer and the second computer and exchanging security credentials over the reliable communication path.

3. The method of claim 2, wherein the step of exchanging security credentials comprises the step of exchanging an encryption key that is used to encrypt the data records in step (2).

4. The method of claim 2, wherein the session information includes at least a portion of the security credentials.

5. The method of claim 1, wherein step (2) comprises the step of incorporating a nonce in each data record that is used by the second computer in combination with a previously shared encryption key to decrypt each of the data records in step (3).

6. The method of claim 5, wherein the nonce comprises a random number.

7. The method of claim 5, further comprising the step of, in the second computer, verifying that the nonce has not previously been received in a previously transmitted data record.

8. The method of claim 1,

wherein step (2) comprises the step of embedding an indicator in each of the data records indicating that the data records are encrypted according to an encryption scheme that encrypts records without regard to any previously transmitted data records, and

wherein step (3) comprises the step of determining whether the indicator is present in each record and, in response to determining that the indicator is not present, processing each such record differently than if the indicator is set.

9. The method of claim 1, wherein step (1) is performed using the Transmission Control Protocol, and wherein step (2) is performed using the User Datagram Protocol.

10. The method of claim 1, wherein step (2) is performed by a proxy server that encrypts data records received from another server.

11. The method of claim 1, wherein the third computer

establishes a communication path with the first computer; and

encrypts and transmits data records to the first computer using an unreliable communication protocol, wherein each data record is encrypted without reference to a previously transmitted data record and by employing the session information.

12. The method of claim 1, wherein a fourth computer

retrieves the session information from the third computer,

establishes a communication path with the first computer; and

encrypts and transmits data records to the first computer using an unreliable communication protocol, wherein each data record is encrypted without reference to a previously transmitted data record and by employing the session information.

13. The method of claim 1, wherein the session information is SSL or TLS session information.

14. The method of claim 1, wherein the session information includes a SSL or TLS session identifier.

15. The method of claim 1, wherein the session information includes an encryption key that is used to encrypt data records in step (2).

16. The method of claim 1, wherein the session information is stored by the third computer in a cache memory using a hash function.

17. The method of claim 16, wherein the hash function is the BUZhash function.

18. The method of claim 1, wherein the second computer transmits the session information to the third computer using multicast communication.

19. The method of claim 18, wherein the multicast communication is negative acknowledgement multicast communication.

20. A method of securely transmitting a plurality of data records between a client computer and a proxy server using an unreliable communication protocol, comprising the steps of:

(1) establishing a reliable connection between the client computer and the proxy server;

(2) exchanging encryption credentials between the client computer and the proxy server over the reliable connection;

(3) generating a nonce for each of a plurality of data records, wherein each nonce comprises an initialization vector necessary to decrypt a corresponding one of the plurality of data records;

(4) using the nonce to encrypt each of the plurality of data records and appending the nonce to each of the plurality of data records;

(5) transmitting the plurality of data records encrypted in step (4) from the client computer to the proxy server using an unreliable communication protocol;

(6) in the proxy server, decrypting each of the plurality of encrypted data records using a corresponding nonce extracted from each data record and a previously shared encryption key; and

(7) in the proxy server, transmitting session information including the previously shared encryption key for use in decrypting the plurality of data records to another server.

21. The method of claim 20, wherein step (6) comprises the step of checking to determine whether each data record received from the client computer is formatted according to a secure unreliable transmission format and, if a particular record is not formatted according to a secure unreliable transmission format, bypassing decryption of the received data record using the corresponding nonce.

22. The method of claim 20, wherein step (3) comprises the step of generating a random number as each nonce.

23. The method of claim 20, wherein step (3) comprises the step of generating an unique number as each nonce.

24. The method of claim 20, wherein step (1) is performed using Transmission Control

Protocol, and wherein step (5) is performed using User Datagram Protocol.

25. The method of claim 20, wherein step (6) is performed using an encryption key previously shared using a reliable communication protocol.

26. The method of claim 25, wherein the reliable communication protocol is Transmission Control Protocol.

27. The method of claim 20, wherein the another server is a second proxy server.

28. The method of claim 27, further including, in the second proxy server, decrypting encrypted data records from the client computer using a corresponding nonce extracted from each data record and the session information transmitted from the first proxy server.

29. The method of claim 20, wherein the another proxy server is a cache memory server.

30. The method of claim 29, further including, in a second proxy server,

obtaining the session information from the cache memory server, and

decrypting encrypted data records from the client computer using a corresponding nonce extracted from each data record and the session information.

31. The method of claim 20, wherein the session information is SSL or TLS session information.

32. The method of claim 20, wherein the session information includes a SSL or TLS session identifier.

33. The method of claim 20, wherein the session information includes authentication information for a user of the client computer.

34. The method of claim 20, wherein the session information is stored by the another server in a cache memory using a hash function.

35. The method of claim 34, wherein the hash function is the BUZhash function.

36. The method of claim 20, wherein the proxy server transmits the session information to the another server using multicast communication.

37. The method of claim 36, wherein the multicast communication is negative acknowledgement multicast communication.

38. A system for securely transmitting data using an unreliable protocol, comprising:

a first computer having a communication protocol client function operable in conjunction with an application program to transmit data records securely using an unreliable protocol; and

a second computer coupled to the first computer and having a communication protocol server function operable in conjunction with the communication protocol client function to receive data records securely using the unreliable communication protocol,

wherein the communication protocol client function encrypts each data record using a nonce and an encryption key and appends the respective nonce to each of the encrypted data records; and

wherein the communication protocol server function decrypts each of the data records using the respectively appended nonce and the encryption key; and

a third computer coupled to the second computer and having a cache memory for storing at least the encryption key.

39. The system of claim 38, wherein the communication protocol client function exchanges encryption credentials with the communication protocol server function using a reliable communication protocol.

40. The system of claim 39, wherein the unreliable communication protocol includes the

User Datagram Protocol, and wherein the reliable communication protocol includes the Transmission Control Protocol.

41. The system of claim 38, wherein the communication protocol client function and the communication protocol server function are compatible with the SOCKS communication protocol.

42. The system of claim 38, wherein the communication protocol client function and the communication protocol server function are compatible with the SSL/TLS communication protocol.

43. The system of claim 38, wherein the second computer comprises a proxy server that forwards decrypted records received from the first computer to a server computer.

44. The system of claim 38, wherein the second computer comprises a record detector that determines whether an indicator has been set in each data record received from the first computer and, if the indicator has not been set for a data record, bypassing decryption of that data record by the communication protocol server function.

45. The system of claim 38, wherein the third computer is a proxy server that

can receive encrypted records from the first computer;

can decrypt records the received records using at least the encryption key stored in the cache memory; and

can forward the decrypted records received from the first computer to a server computer.

46. The system of claim 38, wherein the third computer is a memory cache server, and further including a fourth computer that can

obtain the at least the encryption key stored in the cache memory of the third

computer;

receive encrypted records from the first computer;

decrypt records the received records using at least the encryption key stored in the cache memory; and

forward the decrypted records received from the first computer to a server computer.

47. A method of transmitting securely over a computer network, comprising:

establishing a communication path with a first computer;

receiving data records from the first computer that have been

encrypted such that each data record is encrypted without reference to a previously encrypted data record, and

transmitted using an unreliable communication protocol;

decrypting the encrypted data records without reference to a previously received data record; and

transmitting session information for decrypting the encrypted data records to a second computer.

48. The method of claim 47, further comprising:

establishing a reliable communication path with the first computer prior to receiving the encrypted data records,

and exchanging security credentials with the first computer over the reliable communication path.

49. The method of claim 47, further comprising decrypting each encrypted data record

using a nonce incorporated into the data record in combination with a previously shared encryption key.

50. The method of claim 49, wherein the nonce includes a random number.

51. The method of claim 50, further comprising verifying that the nonce incorporated in the encrypted data record has not been incorporated in a previously received encrypted data record.

52. The method of claim 47, further comprising:

determining whether each data record received from the first computer includes an encryption indicator indicating that the received data record is encrypted, and if the indicator is not present in a received data record, bypassing decryption of that data record

53. The method of claim 47, further comprising

establishing the communication path with the first computer using the Transmission Control Protocol, and

receiving the encrypted data records using the User Datagram Protocol.

54. The method of claim 47, wherein the first computer is a proxy server that encrypts data records received from a third computer.

55. The method of claim 47, wherein the session information is SSL or TLS session information.

56. The method of claim 47, wherein the session information includes an encryption key used to encrypt the received encrypted data records.

57. The method of claim 47, wherein the session information is stored by the second computer in a cache memory using a hash function.

58. The method of claim 47, further comprising transmitting the session information to the second computer using multicast communication.

APPENDIX B - EVIDENCE

None.

APPENDIX C - DECISIONS IN RELATED PROCEEDING

None.